UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/936,157 | 09/06/2001 | Osamu Shibata | NAKI-BP89 | 9192 |

21611 7590 02/12/2004

SNELL & WILMER LLP
1920 MAIN STREET
SUITE 1200
IRVINE, CA 92614-7230

| EXAMINER | |
|---|---|
| MOORTHY, ARAVIND K | |
| **ART UNIT** | **PAPER NUMBER** |
| 2131 | |

DATE MAILED: 02/12/2004 10

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. 09/936,157 | Applicant(s) SHIBATA ET AL. | |
|---|---|---|---|
| | Examiner Aravind K Moorthy | Art Unit 2131 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *17 November 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) *13-16* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12 and 17-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 September 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

## DETAILED ACTION

1. Claims 1-20 are pending in the application.

2. Claims 1-12 and 17-20 have been rejected.

3. Claims 13-16 have been cancelled.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

**4. Claims 1-3, 8-12, and 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Witt et al U.S. Patent No. 5,745,571.**

As to claims 1, 11, 12, 17 and 19, Witt et al discloses a first authentication phase in which the access device transmits to the storage medium scrambled access information generated by scrambling access information which shows the area [column 3 line 61 to column 4 line 4]. Witt et al discloses that it authenticates whether the storage medium is authorized according to a

challenge-response authentication protocol using the scrambled access information [column 4, lines 23-57]. Witt et al discloses a second authentication phase in which the storage medium authenticates whether the access device is authorized [column 4, lines 58-66]. Witt et al discloses a transfer phase in which, when the storage medium and the access device have authenticated each other as authorized devices, the storage medium extracts the access information from the scrambled access information that was used in the authentication protocol. Witt et al discloses that the access device reads/writes digital information from/into the area shown by the access information [column 5 line 28 to column 6 line 3].

As to claims 2 and 18, Witt et al discloses an access information acquisition unit for acquiring the access information that shows the area [column 6, lines 4-24]. Witt et al discloses a random number acquisition unit for acquiring a random number. Witt et al discloses a generation unit for generating random number access information by combining the access information and the random number. Witt et al discloses an encryption unit for encrypting the random number access information according to an encryption algorithm, to generate the scrambled access information, the storage medium includes a response value generation unit for generating a response value from the scrambled access information, and the access device includes an authentication unit for authenticating whether the storage medium is authorized using the response value [column 5, lines 29-45].

As to claims 3 and 20, Witt et al discloses a decryption unit for decrypting the scrambled access information according to a decryption algorithm to obtain the random number access information. Witt et al discloses a separation unit for separating the access information from the random number access information [column 4 line 58 to column 5 line 28].

As to claim 8, The authentication communication system of Claim 3, wherein in the transfer phase, the storage medium, which stores digital information in the area, includes an encryption unit for reading the digital information from the area shown by the access information and encrypting the digital information according to an encryption algorithm to generate encrypted digital information, and the access device, which reads the digital information from the area, includes a decryption unit for decrypting the encrypted digital information according to a decryption algorithm to obtain the digital information, the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm [column 5 line 28 to column 6 line 3].

As to claim 9, Witt et al discloses a digital information acquisition unit for acquiring the digital information. Witt et al discloses an encryption unit for encrypting the digital information according to an encryption algorithm to generate encrypted digital information [column 4, lines 5-22]. Witt et al discloses that the storage medium includes a decryption unit for decrypting the encrypted digital information according to a decryption algorithm to obtain the digital information. Witt et al discloses writing the digital information into the area shown by the access information. Witt et al discloses the decryption algorithm being an algorithm for decrypting a cryptogram generated according to the encryption algorithm [column 4 line 58 to column 5 line 28].

As to claim 10, Witt et al discloses a digital information acquisition unit for acquiring the digital information. Witt et al discloses a content key acquisition unit for acquiring a content key. Witt et al discloses a first encryption unit for encrypting the acquired content key according to a first encryption algorithm to generate an encrypted content key. Witt et al discloses a second

encryption unit for encrypting the encrypted content key according to a second encryption algorithm to generate a double- encrypted content key [column 6, lines 41-65]. Witt et al discloses and a third encryption unit for encrypting the digital information according to a second encryption algorithm using the content key, to generate encrypted digital information. Witt et al discloses that the storage medium includes a decryption unit for decrypting the double encrypted content key according to a first decryption algorithm to obtain the encrypted content key, and writing the encrypted content key into the area shown by the access information, and the storage medium further includes an area for storing the encrypted digital information [column 7, lines 48-59].

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**5. Claims 4-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Witt et al U.S. Patent No. 5,745,571 as applied to claim 1 above, and further in view of Vobach U.S. Patent No. 5,193,115.**

As to claim 4, Witt et al does not teach that in the first authentication phase, the access device further includes a random number seed storage unit for storing a random number seed, and the random number acquisition unit acquires the random number by reading the random number seed from the random number seed storage unit.

Vobach teaches a random number seed storage unit for storing a random number seed, and the random number acquisition unit acquires the random number by reading the random number seed from the random number seed storage unit [column 9, lines 21-39].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Witt et al so that the random number are created with a random number seed that is stored in a storage unit. The random numbers would have been acquired from the storage unit.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Witt et al by the teaching of Vobach because the masking tape string only appears to an eavesdropper as a summand of the known ciphertext string, reconstructing it depends upon knowing the plaintext message string. Since, for a given encrypted message, there will be many equally probably possible plaintext message strings, there will be as many equally probable possible masking tape strings. In short, the plaintext message string "masks" the masking tape string [column 6 line 64 to column 7 line 8].

As to claim 5, the combination of Witt et al and Vobach teaches that in the first authentication phase, the access device further writes the scrambled access information over the random number seed stored in the random number seed storage unit, as a new random number seed [Vobach column 9, lines 40-63].

As to claim 6, the combination of Witt et al and Vobach teaches that in the first authentication phase, the access device further includes a random number seed storage unit for storing a random number seed, and the random number acquisition unit acquires the random number, by reading the random number seed from the random number seed storage unit and

generating the random number based on the random number seed [Vobach column 9, lines 21-63].

As to claim 7, the combination of Witt et al and Vobach teaches that in the first authentication phase, the access device further writes the random number over the random number seed stored in the random number seed storage unit as a new random number seed, as discussed above.

***Conclusion***

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K Moorthy whose telephone number is 703-305-1373. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
February 6, 2004

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100